1187. 整數論ニ於ケル一定理ノ初等的證明ニツイテ

東屋　五郎(名大)

aヲ任意ノ有理整数（以下整数トイヘバ有理整数ノコト），pヲaト素ナル素数トスレバ $a^m \equiv 1 \pmod{p}$ ナル自然数mガ存在シマスガ、mノ中最小ナルモノヲaノ$\bmod p$ニ関スル指数ト呼ビマス。ソレヲnトスレバ n/m デアリマス。特ニ $a^{p-1} \equiv 1 \pmod{p}$ デアル故ニ $n \mid p-1$ 従ツテ$(n, p)=1$ デアリマス。逆ニ任意ニ整数aト自然数nヲ与ヘタトキニaト素ナル素数pノ中aノ$\bmod p$ニ関スル指数ガ丁度nニ等シクナルヤウナpガ存在スルカト云フニ $|a|>1$, $n>2$ナラバ $a=2$, $n=6$; $a=-2$, $n=3$ナル場合ヲ除イテ、カヽルpガ常ニ存在スルトイフ定理ガ成立シマス。

コノ定理ハ実ハ C. Chevalley ・ガ東大　ノ *Sur la théorie du corps de classes dans les corps finis et les corps locaux* (1933)ノ432頁ニ於テ相互律ノ證明ノタメノ補助定理トシテ證明シテ居リマスガ（尤モソレ丈ノ為ナラpノ代リニpノ巾ヲ取ツテ十分デアリ、従ツテソノ場合ノ証明ハ非常ニ簡単ニナルコトヲ彌永先生ガ指摘サレマ

シタガ、高木先生、代数的整数論243頁ノ定理2参照)、ソノ証明ハ透明デハアリマスガ、円分体ノ素「イデヤル」ノ問題ニ迄持ツテ行ツテ居ルノデ、初等的トハ申サレマセン。コヽニソノ初等的ナ証明ガ得ラレマシタノデソレヲ述ベテミマス。Chevalley ノ証明ト比ベテミマシタ所、証明ノ本質ハ同様デアリマス。

nヲ自然数、ζヲ一般ニ1ノ原始n乗根ヲ表ハストキ同同n分多項式

$$(1)\qquad \Phi_n(x)=\prod_{\zeta}(x-\zeta)=\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}$$

ハ$\varphi(n)$次ノ整係数(既約)多項式デアリマス。

$n>2$ノトキハζハ実ナラザル複素数ナル故ζノ共軛複素数ζ^{-1}モ原始n乗根デ、$\zeta^{-1}=\bar{\zeta}$ダカラスラ実数ト考ヘレバ $\Phi_n(x)=\prod_{\zeta}(x-\zeta)=\prod|x-\zeta|=|\Phi_n(x)|$トナリマスガ、$\Phi_n(x)$ハ$x\geqq 1$ニ於テ単調増加、$x\leqq -1$ニ於テ単調減少函数ヲ表ハシマス。

何トナレバ$1\leqq x<y$又ハ$x<y\leqq -1$ナラバ$|\zeta|=1$ナルコトカラ$|x-\zeta|<|y-\zeta|$、従ツテ

$\Phi_n(x)=\prod_{\zeta}|x-\zeta|<\prod_{\zeta}|y-\zeta|=\Phi_n(y)$ナル故デアリマス。

補題1. nガ2ヨリ大ナル自然数、xガ$|x|\geqq 2$ナル実数ナラバ、nノ任意ノ素因数pニ対シテ、

$\Phi_n(x) > p$ デアル。但シ $x=2, n=6$ ナル場合及ビ $x=-2, n=3$ ナル場合ヲ除ク。

証明：　上述ノ $\Phi_n(x)$ ノ単調性ヨリ、$x=\pm 2$ ナル場合ヲヤレバ十分デアルガ、

1)　n ガ平方因子ヲ有シナイ場合

イ)　$n=p$ ガ奇素数ノトキ、$\Phi_n(x)=\frac{x^p-1}{x-1}=x^{p-1}+\cdots+x+1$ トナル故 $\Phi_n(2)>\Phi_n(1)=p$，又 $\Phi_n(-2)=\frac{2^p+1}{3}$ ハ $p>3$ ナラバ $>p$ デアルガ $p=3$ ノトキダケハ $\Phi_3(-2)=3$．シカシ、$x<-2$ ナラバ $\Phi_3(x)>3$ デアル。

ロ)　n ガ素数ナラザル奇数ノトキ、$n=p_1 p_2 \cdots p_s$，$p_1>p_2>\cdots>p_s\ (>2)$，$(s\geqq 2)$ ヲ n ノ素因子分解トシ、$n'=p_1\cdots p_{s-1}$ トオケバ (1) カラ容易ニ

$$\Phi_n(x)=\frac{\Phi_{n'}(x^{p_s})}{\Phi_{n'}(x)}$$

従ッテ

$$\Phi_n(\pm 2)=\frac{\Phi_{n'}(\pm 2^{p_s})}{\Phi_{n'}(\pm 2)}$$

ヲ得ルガ ζ' ヲ一般ニ原始 n' 乗根トセバ

$$\Phi_{n'}(\pm 2^{p_s})=\prod_{\zeta'}|\pm 2^{p_s}-\zeta'|\geqq(2^{p_s}-1)^{\varphi(n')}\geqq 6^{\varphi(n')}$$

$$\Phi_{n'}(\pm 2)=\prod_{\zeta'}|\pm 2-\zeta'|\leqq 3^{\varphi(n')}$$ トナル故ニ

$$\Phi_n(\pm 2)\geqq\frac{6^{\varphi(n')}}{3^{\varphi(n')}}=2^{\varphi(n')}>p_1$$

ハ)　n ガ偶数ノトキ、$n=2n'$ トオケバ、n ガ平方因子ヲ有シナイ仮定カラ n' ハイ)，ロ) ノ場合ノ n トナル故 $n'=3$，$-x=-2$　従ッテ $n=6$，

$x=2$ ノ場合ヲ除イテ n ノ任意ノ素因子 p ニ対シ

$$\Phi_n(x) = \Phi_{n'}(-x) > p$$

ガ成立ツ。

2) n ガ平方因子ヲ有スル場合

イ) n ガ2ノ巾即チ $n=2^e\ (e\geqq 2)$ ナル形ノトキハ $\Phi_n(x)=x^{2^{e-1}}+1$ ナル故，$|x|>1$ ナラ

$$\Phi_n(x) > \Phi_n(\pm 1) = 2$$

ロ) n ガ2以外ノ素因数ヲ含ムトキ．n ノ素因子分解ヲ $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}\ (s\geqq 1)$ トスレバ $p_1^{e_1-1}p_2^{e_2-1}\cdots p_s^{e_s-1}>1$. シカルニ(1)カラ容易ニ $\Phi_n(x)=\Phi_{p_1\cdots p_s}(x^{p_1^{e_1-1}\cdots p_s^{e_s-1}})$ ナル恒等式ヲ得ル故上記イ)ノ場合ニヨリ

$$\Phi_n(x) > \Phi_{p_1\cdots p_s}(x) \geqq p_i \quad (|x|\geqq 2)$$

(証明終)

補題2. a ガ整数，p ガ素数デ、且ツ $p^\nu \| a-1, (\nu\geqq 1)$ トスレバ $p=2$, $\nu=1$ ナル場合ヲ除イテ、$p^{\nu+1}\| a^n-1$ デアル、又 n ガ p ト素ナル自然数ナラバ $p^\nu\| a^n-1$ デアル。($p^\nu\| a-1$ トハ $a-1$ ノ p 成分ガ p^ν ナルコト)

証明：$a=1+b$ トオケバ $p^\nu\| b$ デアル。シカラバ

$$a^p-1 = pb+\binom{p}{2}b^2+\cdots+\binom{p}{p-1}b^{p-1}+b^p$$

トナルガ右辺ノ最初ノ項ハ $p^{\nu+1}\| p^b$ ノ最後ノ項ハ

$p^{p\nu} \| b^p$ デアリ、ソノ他ノ項ハ明ラカニ $p^{\nu+2}$ デ割リ切レル。而シテ $p=2$, $\nu=1$, ノトキヲ除イテハ、$\nu+1<p\nu$ トナル故ニ $p^{\nu+1} \| a^p-1$ ヲ得ル。

次ニ $(n,p)=1$ ノトキ

$$a^n-1 = nb+\binom{n}{2}b^2+\cdots+\binom{n}{n-1}b^{n-1}+b^n$$

デアルガ：右辺ノ最初ノ項ハ $p^\nu \| nb$ デ、ソノ他ノ項ハ明ラカニ $p^{\nu+1}$ デ割リ切レル故 $p^\nu \| a^n-1$ デアル。

補遺3. 整数 a ガ与ヘラレタトキ素数 p ガ a ト互ヒニ素デ且ツ a ノ $\bmod p$ ニ関スル指数ガ n ニ等シイタメノ必要且ツ十分ナル條件ハ、

$$p \mid \Phi_n(a) \text{ 且ツ } p \nmid n$$

ナルコトデアル。

証明： 先ヅ必要條件： $p \mid a^n-1 = \prod_{d \mid n} \Phi_d(a)$ ナル故 $p \mid \Phi_d(a)$ ノ $d \mid n$ トスレバ、$a^d \equiv 1 \pmod p$ デアルカラ $d \geqq n$, 從ツテ $d=n$ 即チ $p \mid \Phi_n(a)$, 勿論 $p \nmid n$ デアル。

次ニ十分條件： $p \mid \Phi_n(a)$, $p \nmid n$ トセバ $a^n \equiv 1 \pmod p$ デアルガ、a ノ $\bmod p$ ニ関スル指数ヲ f トオケバ $f \mid n$ デアル。

今 $p^\nu \| a^f-1$ $(\nu \geqq 1)$ トオケバ $(\frac{n}{f}, p)=1$ ナル故上ノ補題2カラ $p^\nu \| a^n-1$ 從ツテ若シ $n>f$ ナ

ラバ $p^{\nu+1} | \Phi_n(a)\cdot(a^f-1) | a^n-1$ トナリ矛盾スル故

$n=f$ デアル。

補題4. a ハ整数、p ハ a ト互ニ素ナル素数デ且ツ a ノ $\bmod p$ ニ関スル指数ガ f ナルトキ $p|\Phi_n(a)$ オルタメノ必要且ツ十分ナル條件ハ、n ガ $n=p^e f$ $(e\geqq 0)$ ナル形ニ表ハサレルコトデアル。

而シテソノ場合、$n>f$, $n\neq 2$ ナラバ $p\|\Phi_n(a)$ デアル。

證明: 先ヅ必要條件: $p^e\| n$ トセバ $p\nmid f|n$ ナル故、$p^e f|n$ デアルカラ、 $n=p^e f n'$ トオケバ $p\nmid n'$.

従ツテ、$p^\nu\| a^{p^e f}-1$ トオケバ、補題2ヨリ $p^\nu\| a^n-1$ デアル故、若シ $n>p^e f$ ナラ $p^{\nu+1}|\Phi_n(a)\cdot(a^{p^e f}-1)|a^n-1$ トナリ矛盾スル。従ツテ $n=p^e f$ 逆ニ十分條件: $n=p^e f$ $(e\geqq 0)$ ナル形デアルトスル。$e=0$ 即チ $n=f$ ナラバ、補題3カラ $p|\Phi_n(a)$ ヲ得ル。ソユデ $e\geqq 1$ 即チ $n>f$ ノ場合ヲ考ヘル。

$$p^\nu\| a^{p^{e-1}f}-1=\prod_{\delta|f}\Phi_\delta(a),\quad (\nu\geqq 1)$$

トオケバ、補題2ニヨレバ $p=2, \nu=1$ ナル場合ヲ除イテ

$$p^{\nu+1}\| a^{p^e f}-1=\prod_{d|p^e f}\Phi_d(a)$$

得ル故、コノ二式ヲ比較シテ、$p\|\Phi_d(a)$, $d\nmid p^e f$.

$d \times p^{e-1} f$ ナル d ガ唯一ツ存在シナケレバナラナイコトガ分カル。コノ d ハ $d = p^e d'$ $d' | f$ ナル形ニ表ハサレルガ、$a^d \equiv 1 \pmod{p}$ ナル故ニ、$f | d = p^e d'$ デナケレバナラナイガ、$(f', p) = 1$ ナル故、$f | d'$, 従ツテ $f = d'$, $d = p^e f = n$ 即チ $p \| \Phi_n(a)$ トナル。

$p = 2$, $\nu = 1$ ナル場合ハ $f | p - 1 = 1$ ナル故 $f = 1$, 従ツテ $n = 2^e$ デアルガ、$e > 1$ ナラバ $4 | a^{2^e} - 1$ ナル故 $\nu > 1$ トナルカラ $e = 1$, 即チ $n = 2$ デナケレバナラナイ。

コノ場合モ確カニ $2 | \Phi_2(a) = a + 1$ デアル。

以上ノ補題ヲ使ツテ、求ムル定理ガ簡単ニ証明サレル。

定理、 aハ $|a| > 1$ ナル整数, nハ2ヨリ大ナル自然数トスレバ、aト互ヒニ素ナル素数pノ中デ、aノ mod p ニ関スル指数ガ丁度 n ニ等シクナルヤウナpガ少クトモ一ツ存在スル。但シ $a = 2$, $n = 6$ ナル場合及ビ $a = -2$, $n = 3$ ナル場合ヲ除ク。

証明： 補題2ニヨレバ、$p | \Phi_n(a)$ 且ツ $p \nmid n$ ナルpノ存在ヲイヘバヨイワケデアル。ソコデ若シ、然ラズトスル、即チ $p | \Phi_n(a)$ ナラバ $p | n$ ガ成立ツトスル。ソノpヲトリ a ノ mod p ニ関スル指数ヲ f トオケバ、$n > f$ デ、$n > 2$ デアルカラ、補題4ニ

ヨツテ、

$$n = p^e f, \quad p \| \Phi_n(a)$$

デナケレバナラナイ。

シカルニ $f \mid p-1$ ナル故 $f < p$ 従ツテ p ハ n ノ最大素因数トナル故、$\Phi_n(a)$ ハ p 以外ノ素因数ヲ有シナイコトニナリ、結局 $\Phi_n(a) = p$ デナケレバナラナイコトニナルガ、コレハ補題1ニヨレバ、二ツノ例外ノ場合ヲ除イテハ不可能デアル。